

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND**

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT AND
CRIMINAL COMPLAINT**

UNDER SEAL
JAN 03 2019
U.S. DISTRICT COURT
DISTRICT OF MARYLAND
DEPUTY

I, Rachel Corn, being duly sworn, depose and state as follows:

1. This affidavit is submitted in support of an application for warrants to search the following locations (the "TARGET LOCATIONS"):
 - a. The digital devices seized from the person and residence of Kevin Daniel Mongold, Jr, on October 24, 2018, described more fully in Attachment A1;
 - b. The associated files of **Cybertipline Reports 11860995** and **11861015** that were forwarded to the National Center for Missing and Exploited Children (NCMEC) by Facebook, described more fully in Attachment A2 ;
 - c. The associated files of **Cybertipline Reports 42610198** and **42611405** that were forwarded to the National Center for Missing and Exploited Children (NCMEC) by Box.com, described more fully in Attachment A2;
 - d. The Facebook account associated with the email address **keviejrmongold@yahoo.com** and the ESP User ID: 100010728783044, described more fully in Attachment A3;
 - e. The Facebook account associated with the email address **kevin.mongold19@yahoo.com**, the ESP User ID: 100012201795245, and screen name: kevin.mongold.56, described more fully in Attachment A3;
 - f. The Facebook account associated with the email address **mongoldjr.kevin@gmail.com** and the ESP User ID: 100017871872850, described more fully in Attachment A3;
 - g. The Oath Holdings account associated with **keviejrmongold@yahoo.com**, described more fully in Attachment A4;
 - h. The Oath Holdings account associated with **kevin.mongold19@yahoo.com**, described more fully in Attachment A4;
 - i. The Oath Holdings account associated with **mongoldjim@yahoo.com**, described more fully in Attachment A4;
 - j. The Dropbox account associated with the email address **mongoldjr.kevin@gmail.com** and the ESP User ID: 721902735, described more fully in Attachment A5;

18 - 3486 JMC — **18 - 3494 JMC**

k. The Google account associated with the email address **mongoldjr.kevin@gmail.com**, described more fully in Attachment A6;

l. The Google account associated with the email address **mongoldjim@gmail.com**, described more fully in Attachment A6;

m. The Google account associated with the email address **mongold.kevin@gmail.com**, described more fully in Attachment A6;

n. The Google account associated with the email address **mongold.kevin1997@gmail.com**, described more fully in Attachment A6;

o. The Box.com account associated with the email address **mongoldjr.kevin@gmail.com** and the ESP User ID: 2974294259, described more fully in Attachment A7;

p. The Box.com account associated with the email address **mongoldjim@gmail.com**, described more fully in Attachment A7;

q. The Apple account associated with the email address **mongoldjim@gmail.com** and DS ID 10032188562, described more fully in Attachment A8 ;

r. The Apple account associated with the email address **mongoldjim@yahoo.com** and DS ID: 10031960637, described more fully in Attachment A8; and

s. The Apple account associated with the email address **mongold.kevin@gmail.com** and DS ID: 415693081, described more fully in Attachment A8.

2. This affidavit is also made in support of a criminal complaint and arrest warrant for Kevin Daniel Mongold, Jr (“Mongold”), born in 1997, 5403 Highridge Street, Halethorpe, Maryland 21227, for violation of Title 18, United States Code, Section 2251(a) (production of child pornography).

3. I submit that there is probable cause to believe that the TARGET LOCATIONS will contain evidence of Title 18, United States Code, Section 2251(a) (production of child pornography), Title 18, United States Code, Section 2252A(a)(2) (distribution and receipt of child pornography), and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography) (the “TARGET OFFENSES”).

18 - 3486 JMC**18 - 3494 JMC****AGENT BACKGROUND**

4. I am a Special Agent with the Federal Bureau of Investigation (FBI), Baltimore Division, Baltimore, Maryland. I have been a SA with the FBI since May 2006. Since September 2006, I have primarily investigated federal violations concerning child pornography and the sexual exploitation of children. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received FBI Crimes Against Children training, FBI Innocent Images Online Undercover training, and FBI Peer-to-Peer Network Online Investigation training. I have participated in the execution of numerous search warrants, of which the majority have involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violations of federal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with the FBI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

5. The statements in this affidavit are based in part on information and reports provided by Baltimore County Police Department, NCMEC, Dropbox, Facebook, Box.com and Special Agents of the FBI, and on my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set

forth only the facts that I believe are necessary to establish probable cause to believe I have set forth only the facts that I believe are necessary to establish probable cause to believe that Mongold has committed criminal violations of 18 U.S.C. § 2251(a) (production of child pornography), and that evidence, fruits, and instrumentalities of the TARGET OFFENSES are located in the TARGET LOCATIONS.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO PRODUCE, POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE PRODUCTION, POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

6. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures,

18 - 3 4 8 6 JMC — **18 - 3 4 9 4 JMC**

films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

h. I also know that the location of mobile phones can provide information about the individual's whereabouts, showing the places the holder resides or travels to, including the locations of additional digital devices that the individual possesses, controls, and has access to.

7. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images.

18 - 3486 JMC

18 - 3494 JMC

As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers, smartphones and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of the residence.

d. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer, via a USB cable, and transfer data files from one digital device to another. Many people generally carry their smartphone on their person.

e. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

f. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

g. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online

18 - 3 4 8 6 JMC

18 - 3 4 9 4 JMC

communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

h. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, there exists a fair probability that evidence regarding the distribution, receipt and possession of child pornography will be found in the TARGET LOCATIONS notwithstanding the passage of time.

j. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

k. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

l. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

m. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

n. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above-described information will be recovered during forensic analysis.

NCMEC CYBERTIPLINE

18 - 3 4 8 6 JMC — 18 - 3 4 9 4 JMC

8. The National Center for Missing and Exploited Children (NCMEC) receives complaints via their Cybertipline from Internet Service Providers (ISPs), Electronic Service Providers (ESPs), and others. These Cybertipline reports are reviewed by a NCMEC analyst and forwarded to law enforcement for further investigation on the information provided in the Cybertipline report.

KIK

9. Kik a smartphone messenger application available for most iOS, Android, and Windows Phone operating systems. Kik Messenger lets users send text, pictures, videos, sketches, and other files within the Kik app. Kik is free to download and uses an existing Wi-Fi connection or data plan to send and receive messages. Kik uses usernames to identify their users. A Kik username is the only unique identifier in the Kik system, and the only way Kik can identify a unique Kik account. Kik can be used to message an individual user or a group of users. Kik Interactive is located In Ontario, Canada. Kik only retains IP addresses for the past 30 days.

FACEBOOK

10. Facebook is a free social networking website that provides a host of services to its users. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. Facebook users can post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. A particular user’s profile page includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links.

11. Facebook has a Photos application, where users can upload images and videos. Another feature of the Photos application is the ability to “tag” (i.e., label) other Facebook users

18 - 3486 JMC

18 - 3494 JMC

in a photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

12. Facebook users can exchange private messages with one another. These messages, which are similar to email messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

13. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook also has a Marketplace feature, which allows users to post free classified ads, including items for sale, housing, jobs, and the like.

OATH HOLDINGS ACCOUNT

14. Yahoo provides numerous free services to the users with a Yahoo account. Some of the services include Mail, Flickr, and Messenger. Yahoo Mail is a web-based email service that can also be accessed via a mobile app. In 2017, Yahoo email comes with 1TB of free storage and users can send and receive emails up to 25 megabytes in size, including attachments. Emails remain in an active Yahoo account until deleted by the user. Flickr is an image and video hosting website that offers private and public image storage. A user uploading an image can set privacy controls that determine who can view the image. Yahoo Messenger is an instant

18 - 3 4 8 6 JMC — 18 - 3 4 9 4 JMC

messaging service that provides text and voice communication. Users can also share files and images through the Messenger service. Yahoo only retains user logs and account information for one calendar year. Yahoo Holdings, Inc. is now known as Oath Holdings, Inc.

DROPBOX

15. Dropbox is a file hosting service that offers “cloud” storage and file synchronization. Dropbox offers free and paid services that allow users to add photos, documents, videos and files to their account. Dropbox automatically saves these files to all of the user’s computers, phones and to the Dropbox server, so they may be accessed from anywhere. Dropbox offers a free plan that allows users to have 2GB of space to store their files. Dropbox also offers additional space on the Dropbox servers for a fee.

16. According to Dropbox’s privacy policy, at <https://www.dropbox.com/privacy>, Dropbox collects and stores the files users upload and delete and also collects logs. Dropbox records when the user uploads and deletes a file but Dropbox does not record when the user downloads a file. Dropbox collects and associates a user’s account with their name, email address, phone number, payment info, physical address, and account activity. Dropbox collects information related to how users use their Services, including actions users take in their account, like sharing, editing, viewing, and moving files or folders. Dropbox also collects information from and about the devices users use to access their Services. This includes things like IP addresses, the type of browser and device used, the web page visited before coming to Dropbox sites, and identifiers associated with the users’ devices.

17. In order to create a Dropbox account, a user is required to register with an email address. Once registered, each user is assigned a unique user ID. Dropbox communicates with users via stored email accounts on file when users access and make changes to their accounts

18 - 3486 JMC

18 - 3494 JMC

unless the user opts-out of those emails. To sign into the user's Dropbox account, the user enters their email and password. Once a user has a Dropbox account, they can invite other Dropbox users to access their shared folders. A shared folder is one in which more than one user has access to, and can add, download or delete content. If a user joins another user's shared folder, the shared folder size counts towards the first user's space limitation. If a user is invited to join another user's folder, the invitation request is sent to the registered email account.

APPLE

18. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). The services include email, instant messaging, and file storage.

19. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

20. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents.

18 - 3486 JMC 18 - 3494 JMC

iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

21. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for Kik, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud.

GOOGLE ACCOUNT

22. Google provides numerous free services to the users with a Google profile. Some of services include, Gmail, Google Hangouts, Google Wallet, Google+, Google Drive, Picasa Web Albums, and YouTube. Gmail is a web-based email service that can also be accessed via mobile apps. In 2017, Gmail comes with 15GB of free storage and users can receive emails up

18 - 3 4 8 6 JMC

18 - 3 4 9 4 JMC

to 50 megabytes in size, including attachments, while they can send emails up to 25 megabytes. In order to send larger files, users can insert files from Google Drive into the message. Emails remain in an active Gmail account until deleted by the user. Google Hangouts is a communication platform which includes instant messaging, video chat, and SMS and Voice Over IP (VOIP) features service that provides both text and voice communication. Google Hangouts allows conversations between two or more users. Chat histories are saved online, allowing them to be synced between devices. Google Wallet is a mobile payment system that allows its users to store debit cards, credit cards, loyalty cards and gift cards, among other things, on their mobile phones. Google+ is a social networking service. Google Drive is a file storage and synchronization service, which provides users with cloud storage, file sharing, and collaborative editing. Picasa Web Albums is an image hosting and sharing web service that allows users with a Google account to store and share images for free. YouTube is a free video sharing website that allows users upload, view and share videos.

BOX

23. Box is a cloud content management and file sharing service. Box provides file-sharing, collaborating, and other tools for working with files that are uploaded to its servers. Users can determine how their content can be shared with other users. Users may invite others to view and/or edit an account's shared files, upload documents and photos to a shared files folder (and thus share those documents outside Box), and give other users rights to view shared file. Box offers free and paid accounts.

PROBABLE CAUSE

2016 Facebook Cybertipline Investigation:

24. On May 26, 2016, Facebook sent **Cybertipline Report 11860995** to NCMEC,

18 - 3486 JMC

18 - 3494 JMC

listed the Incident Type as "Child Pornography (possession, manufacture, and distribution)," and listed the incident date as 05/25/2016 at 03:10:31 UTC.

25. The report for 11860995 stated that the Facebook account associated with the email address **keviejrmongold@yahoo.com** and the **ESP User ID: 100010728783044** uploaded two files that were sent to another Facebook user. Within the report, Facebook indicated that they reviewed one of the two files that were uploaded and sent. Facebook provided both files to NCMEC as part of the Cybertipline report.

26. Facebook provided the following information regarding the account:

Name:	Kevin Jr. Mongold
Date of Birth:	XX/XX/1997
Approximate Age:	19
Email Address:	kevinjrmongold@yahoo.com (Verified)
ESP User ID:	100010728783044
Profile URL:	http://www.facebook.com/people/Kevin-Jr-Mongold/100010728783044
IP Address:	76.114.170.98 on 04-30-2016 19:09:33 UTC

27. On May 26, 2016, Facebook sent another Cybertipline Report to NCMEC, **Cybertipline Report 11861015**, and listed the Incident Type as "Child Pornography (possession, manufacture, and distribution)," and 05/25/2016 at 03:35:26 UTC.

28. The report for 11861015 stated that the Facebook account associated with the email address **kevin.mongold19@yahoo.com**, the **ESP User ID: 100012201795245**, and screen name: kevin.mongold.56 uploaded one file that was sent to another Facebook user. Facebook reviewed the one file that was uploaded and sent and provided the file to NCMEC as part of the Cybertipline report.

29. Facebook provided the following information regarding the account:

Name:	Kevin Mongold
Date of Birth:	XX/XX/1997
Approximate Age:	19

18 - 3486 JMC

18 - 3494 JMC

Email Address: **kevin.mongold19@yahoo.com** (Verified)
Screen/User Name: kevin.mongold.56
ESP User ID: **100012201795245**
Profile URL: <http://www.facebook.com/kevin.mongold.56>
IP Address: 2601:143:4200:f620:9d64:ad0b:fbe6:f02 on 05/25/2016

30. Both Cybertipline reports were provided to Baltimore County Police Department for further investigation.

31. A public database query determined that the IP address was managed Comcast. A subpoena was sent to Comcast for the IP address 2601:143:4200:f620:9d64:ad0b:fbe6:f02 for the date and time provided in Cybertipline Report 11861015. Comcast provided records which establish that the IP address was assigned to: Kevin Mongold, 5403 Highridge Street, Halethorpe, Maryland 21227.

32. On July 25, 2016, a Baltimore County Detective interviewed **Kevin Mongold, Jr.**, born in 1997, regarding the Cybertipline reports. Mongold advised that he obtained the image from his Kik account and stated that he thought the female depicted in the image was 18 years old. Mongold was warned by the detective about posting images on social media and Mongold advised he was sorry and it would not happen again. No further investigation was conducted and the case was closed.

2018 Dropbox Cybertipline Investigation:

33. On October 18, 2018, Dropbox sent Cybertipline Report 41922524 to NCMEC, listed the Incident Type as "Child Pornography (possession, manufacture, and distribution)," and listed the date of the incident as 10/17/2018 at 22:57:00 UTC. The report was escalated by NCMEC because it contained image(s) that appeared unfamiliar and may be new or homemade.

34. The report for 41922524 stated that the Dropbox account associated with the email address **mongoldjr.kevin@gmail.com**, the **ESP User ID: 721902735**, and screen name:

18 - 3486 JMC — 18 - 3494 JMC

kevin mongold uploaded 31 files. Dropbox reviewed the 31 files that were uploaded and provided the files to NCMEC as part of the Cybertipline report. A NCMEC analyst viewed the uploaded files and found what appears to be apparent child pornography.

35. NCMEC analysts provided the following information regarding some of the images provided in the Cybertipline report. EXIF metadata within eleven of the submitted images indicated the files may have been produced on May 8, 2018, with an Apple iPhone 7 Plus. GPS coordinates were also found within the EXIF metadata of the eleven images. The NCMEC analyst queried Google for the GPS coordinates and determined that they were all resulting to a baseball field just off of Highridge Street in Halethorpe, Maryland.

36. On October 24, 2018, the Cybertipline report and associated files were provided to both the Baltimore County Police Department and the FBI for further investigation.

37. I reviewed the 31 files associated with Cybertipline report 41922524 and concluded, based on my training and experience, that almost all of the files contain visual depiction of minors engaging in sexually explicit conduct and are child pornography under 18 U.S.C. § 2256(8). In eleven of the pictures, all containing the date "May 8" in their titles, a prepubescent male's penis is exposed to the camera. In one of the pictures, the prepubescent male's face is seen and the background of the picture depicts what appears to be a laundry room. In four of the pictures, an adult hand or finger is also seen touching or near the prepubescent male's penis.

38. On October 24, 2018, investigators were able to locate and interview a prepubescent male, John Doe, born in January 2013. Investigators were able to confirm that John Doe was the same prepubescent male that was depicted in the picture taken in the laundry room containing the prepubescent male's face, which was provided with Cybertipline report

18 - 3486 JMC

18 - 3494 JMC

41922524. John Doe did not disclose information about sexual abuse during the interview.

39. On October 24, 2018, based on the facts detailed above, Baltimore County investigators were able to obtain a state search and seizure warrant for 5403 Highridge Street, Halethorpe, Maryland 21227, and for Kevin Daniel Mongold, Jr's person. On October 24, 2018, Baltimore County and FBI personnel secured the residence while the search warrant was obtained. Present at the residence were Mongold's father, who has the same name, his step-mother, step-brother, and grandmother. It was determined that Mongold was not home at the time. Later on October 24, 2018, Mongold returned home and a black **Apple iPhone** with a cracked screen, **S/N: FCFTC10THG00, Model: A1661**, was seized from Mongold's person as he walked up to the front door of the residence.

40. The black **Apple iPhone, S/N: FCFTC10THG00**, was previewed and three photo vault applications, Family Vault, Keep Safe, and Photo Vault, were located within the cell phone. Mongold provided a passcode to access the photo vault applications and several hundred images and videos of child pornography were located in the applications. In the Photo Vault application, investigators located approximately 49 images and 1 video depicting John Doe in a folder titled with John Doe's first name. The images depicted John Doe naked, with a male's hand pulling down John Doe's shorts and a male's hand touching John Doe's penis. The video file depicted John Doe performing oral sex on an adult male's penis.

41. During the execution of the search warrant, a black **HP Laptop, Model: 15-BS020WM, S/N: CND72915HX**, was located inside a black backpack on the floor of the room identified as Mongold's bedroom. Mongold's bedroom was located in the basement next to the washer and dryer. The washer and dryer appeared to be the same as the background depicted in the image of John Doe provided by Dropbox in Cybertipline report 41922524. A Baltimore

18 - 3 4 8 6 JMC

18 - 3 4 9 4 JMC

County detective conducted a forensic triage of the laptop computer. The 11 images depicting John Doe's penis, which had been provided by Dropbox in Cybertipline report 41922524, were found on the HP laptop computer. In addition to the 11 images, thousands of images and videos of child pornography were located in subfolders under the directory users\kevin mongold\Dropbox.

42. During the execution of the search warrant, Mongold waived his *Miranda* rights and consented to an interview, which was audio recorded. Mongold advised his email address was **mongoldjr.kevin@gmail.com** but that he had not checked his email for approximately five months. Mongold stated that he had a computer that was located in a bookbag in his bedroom. Mongold stated that the last time he used the computer was approximately four months ago. Mongold's cell phone is an Apple iPhone 7. Mongold advised he recently lived in Montana and North Dakota from November 2017 to March 2018 and other people in Montana may have used his computer because it was considered the "apartment computer." Mongold stated that he did not think people at his Montana apartment put child pornography on his computer. Mongold stated that from approximately April 2018 until two to three weeks prior to the search warrant, he primarily resided at his grandparent's house and came back and forth between his grandparent's residence and his father's residence (located on 5403 Highridge Street).

43. Mongold stated that his Facebook account was in the name "**John Carter**." Mongold explained that when he tried to create Facebook accounts in his real name, they were taken down so he created an account in the name John Carter. Mongold stated that he used his Facebook account the morning of the search warrant. Initially Mongold stated that he created a Dropbox account on his computer located in the bookbag and did not upload anything to the account and did not ever use the account. Mongold advised a week after creating the account he

18 - 3 4 8 6 JMC

18 - 3 4 9 4 JMC

thought the account was hacked. He stated that when he tried to log into the Dropbox account, the password would not work. Mongold stated that he thinks the email address associated with the Dropbox account he created was **mongoldjr.kevin@gmail.com**. Later, Mongold advised that he had uploaded thousands of files that were mostly child pornography files to his Dropbox account. Mongold advised that at least one other person from Kik had access to his Dropbox account. Mongold's cell phone sync's to his laptop and Dropbox account.

44. Mongold advised that he does have child pornography files on his computer. Mongold stated he has not looked at the files in approximately four months. Mongold used Kik groups to send and receive the files. Mongold has several Kik usernames. One of the usernames was doggyboy1997. Mongold also uploaded child pornography to a Mega¹ account that was associated with the email **mongoldjim@gmail.com**.

45. Mongold knows John Doe. He stated that he periodically babysat John Doe. Mongold stated that one time John Doe found one of Mongold's pornographic magazines. He stated that John Doe was "curious and got my phone and stuff happened." Mongold stated that he took some of the pictures, and that John Doe took some of the pictures with Mongold's Apple iPhone 7. Mongold stated that he thinks he masturbated John Doe in the pictures. Mongold described two other incidents with John Doe which occurred in Mongold's bedroom at 5403 Highridge Street, Halethorpe, Maryland 21227, over approximately a year. Mongold advised that he performed oral sex on John Doe "a couple times." Mongold advised that John Doe performed oral sex on Mongold one time. Mongold also described a time when John Doe masturbated Mongold. Mongold stated the incidents started approximately two months before he left for Montana. Mongold stated that John Doe was 5 years old during these incidents.

¹ Mega is an internet cloud storage hosting service based in New Zealand.

18 - 3486 JMC — 18 - 3494 JMC

46. Mongold was shown several of the pictures that were provided by Dropbox in Cybertipline report 41922524. Mongold advised it was his hand in the pictures and that either he took the pictures or John Doe took the pictures.

47. On October 24, 2018, Mongold was arrested and charged in Baltimore County, Maryland, with one count of Child Porn Film in Sex Act, Maryland CR.11.207.(a)(2)(3), one count of Possess Child Pornography, Maryland CR.11.208, one count of Sex Abuse Mnr/Cont Course Cond, Maryland CR.3.315, one count of Sex Abuse Minor:House/Fam, Maryland CR.3.602.(b)(2), one count of Sex Offense Third Degree, Maryland CR.3.307, one count of Sex Offense Forth Degree-Sex Contact, Maryland CR.3.308, and one count of Rape Second Degree, Maryland CR.3.304. Mongold has been detained on those charges since his arrest on October 24, 2018.

48. The following is a description of the items seized from Mongold's person or residence on October 24, 2018, which are the subject of this affidavit and application for a search warrant:

- *Black HP Laptop, Model: 15-BS020WM, S/N: CND72915HX*
- *White Apple iPhone, Model: A1453, IMEI: 352000068875701*
- *Black Apple iPhone with cracked screen, S/N: FCFTC10THG00, Model: A1661*
- *Rose Gold Apple iPhone, Model: A1687, S/N: F2M0M633GRWM*
- *Black XBOX 360, Model: 1439, S/N 406639703005*
- *Black Sony Playstation 4, Model: CUH-1115A, S/N: MB315941043*

2018 Box.com Cybertipline Reports

49. On November 2, 2018, Box.com sent **Cybertipline Report 42610198** to NCMEC, listed the Incident Type as "Child Pornography (possession, manufacture, and distribution)," and listed the incident date and time as 10/30/2018 at 21:54:50 UTC.

50. The report for 42610198 stated that the Box.com account associated with the

18 - 3486 JMC — 18 - 3494 JMC

email address **mongoldjr.kevin@gmail.com** and the **ESP User ID: 2974294259** uploaded twenty-two files. Within the report, Box.com did not provide information on whether they had reviewed the files associated with **Cybertipline Report 42610198**. Box.com provided that the files were uploaded from the IP address 216.228.40.58 on 12/06/2017 at 00:26:32 UTC.

51. On November 2, 2018, Box.com sent **Cybertipline Report 42611405** to NCMEC, listed the Incident Type as “Child Pornography (possession, manufacture, and distribution),” and listed the incident date and time as 10/30/2018 at 21:54:50 UTC.

52. The report for 42611405 stated that the Box.com account associated with the email address **mongoldjr.kevin@gmail.com** and the **ESP User ID: 2974294259** uploaded forty-five files. Within the report, Box.com did not provide information on whether they had reviewed the files associated with **Cybertipline Report 42611405**. Box.com provided that the files were uploaded from the IP address 216.228.40.58 on 12/06/2017 at 00:26:32 UTC.

Subscriber Information for Online Accounts

53. A subpoena was served on Facebook requesting subscriber information associated with ESP User ID: 100010728783044. Facebook provided the following information:

Name:	Kevin Jr Jr Mongold
Registration Date:	11/16/2015
Email Address:	keviejrmongold@yahoo.com
Account Closure Date:	05/25/2016

This account was preserved on October 24, 2018.

54. A subpoena was served on Facebook requesting subscriber information associated with ESP User ID: 100012201795245. Facebook provided the following information:

Name:	Kevin Mongold
Registration Date:	05/25/2016
Email Address:	kevin.mongold19@yahoo.com
Account Closure Date:	05/25/2016

18 - 3486 JMC

18 - 3494 JMC

This account was preserved on October 24, 2018.

55. A subpoena was served on Facebook requesting subscriber information associated with the username "John Carter." Facebook provided the following information:

Name:	John Carter
Registration Date:	06/05/2017
Pay Pal Email Address:	mongoldjr.kevin@gmail.com
ESP User ID:	100017871872850

This account was preserved on October 25, 2018.

56. A subpoena was served on Yahoo requesting subscriber information associated with the email address **keviejrmongold@yahoo.com**. Yahoo provided the following information:

Name:	kevie jr mongold
Registration Date:	11/16/2015
Alternate Comm Channel:	4438576180 (Verified)
Account Status:	Active

This account was preserved on October 24, 2018.

57. A subpoena was served on Yahoo requesting subscriber information associated with the email address **kevin.mongold19@yahoo.com**. Yahoo provided the following information:

Name:	kevin mongold
Registration Date:	05/25/2016
Alternate Comm Channel:	4435400843 (Verified)
Account Status:	Active

This account was preserved on October 24, 2018.

58. A subpoena was served on Yahoo requesting subscriber information associated with the email address **mongoldjim@yahoo.com**. Yahoo provided the following information:

Name:	Jim Mongold
Registration Date:	10/23/2012
Zip:	21227

18 - 3486 JMC

18 - 3494 JMC

Account Status: Active

59. A subpoena was served on Kik requesting subscriber information associated with the username "doggyboy1997." Kik provided the following information:

First Name: Steve
Last Name: Rogers
Email Address: **mongold.kevin@gmail.com** (unconfirmed)
Registration TimeStamp: 04/03/2018

60. A subpoena was served on Dropbox requesting subscriber information associated with the email address **mongoldjr.kevin@gmail.com**. Dropbox provided the following information:

Name: kevin mongold
Registration Date: 12/07/2017
User ID: **721902735**
Subscription Status: Free
Account Status: Disabled

This account was preserved on October 24, 2018.

61. A subpoena was served on Google requesting subscriber information associated with the account **mongoldjr.kevin@gmail.com**. Google provided the following information:

Name: kevin mongold
Created On: 05/04/2017
Recovery Email: **mongold.kevin1997@gmail.com**
SMS: 4435400843

This account was preserved on October 24, 2018.

62. A subpoena was served on Google requesting subscriber information associated with the account **mongoldjim@gmail.com**. Google provided the following information:

Name: kevin mongold
Created On: 12/26/2012
Recovery Email: **mongoldjim@yahoo.com**
SMS: 4435400843

This account was preserved on November 1, 2018.

18 - 3486 JMC — 18 - 3494 JMC

63. A subpoena was served on Google requesting subscriber information associated with the account **mongold.kevin@gmail.com**. Google provided the following information:

Name:	Kevin Mongold
Created On:	08/15/2011
Recovery Email:	kmongold@infinityem.com
SMS:	6145060763

64. A subpoena was served on Google requesting subscriber information associated with the account **mongold.kevin1997@gmail.com**. Google provided the following information:

Name:	the song reaper
Created On:	06/29/2016
SMS:	4435400843

65. A subpoena was served on Box.com requesting subscriber information associated with the account **mongoldjr.kevin@gmail.com**. Box.com provided the following information:

Login:	mongoldjr.kevin@gmail.com
Created On:	12/05/2017
Account Type:	Lite (10GB)

This account was preserved on October 25, 2018.

66. A subpoena was served on Box.com requesting subscriber information associated with the account **mongoldjim@gmail.com**. Box.com provided the following information:

Login:	mongoldjim@gmail.com
Created On:	08/03/2018
Account Type:	Lite (10GB)

67. A subpoena was served on Apple requesting subscriber information relating to the email account **mongoldjim@gmail.com**, **mongoldjim@yahoo.com**, and **mongold.kevin@gmail.com**. Apple provided the following information relating to the account:

Apple ID:	mongoldjim@gmail.com
DS ID:	10032188562
Account Type:	Full iCloud
Name:	Kevin Mongold

18 - 3 4 8 6 JMC

— 18 - 3 4 9 4 JMC

Account Status:	Active
Created On:	10/21/2015
Address:	5403 Highridge
City:	Baltimore, Maryland
Day Phone:	4435400843

This account was preserved on November 1, 2018.

Apple ID:	mongoldjim@yahoo.com
DS ID:	10031960637
Account Type:	Full iCloud
Name:	Kevin Mongold
Account Status:	Active
Created On:	10/21/2015
Address:	5403 Highridge
City:	Baltimore, Maryland
Day Phone:	4434716741

Apple ID:	mongold.kevin@gmail.com
DS ID:	415693081
Account Type:	Full iCloud
Logi Alias:	mongold.kevin@icloud.com
Name:	Kevin Mongold
Account Status:	Active
Created On:	11/03/2011
Address:	1855 S County Line Rd
City:	Johnstown, Ohio
Day Phone:	6145060763

CONCLUSION

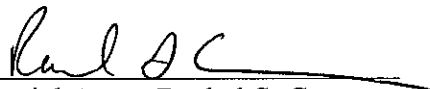
68. Based upon the foregoing information set forth in this application, I respectfully submit that there is probable cause to believe that Kevin Daniel Mongold, Jr, violated Title 18, United States Code, Section 2251(a) (production of child pornography).

69. Also, based on the foregoing information, I have probable cause to believe that contraband, evidence, fruits, and instrumentalities of the TARGET OFFENSES as set forth herein and in Attachments B1, B2, B3, B4, B5, B6, B7, and B8 are currently contained in the TARGET LOCATIONS, more fully described in Attachments A1, A2, A3, A4, A5, A6, A7, and A8. I therefore respectfully request that search warrants be issued authorizing the search of the

18 - 3486 JMC

18 - 3494 JMC

locations described in Attachments A1, A2, A3, A4, A5, A6, A7, and A8 for the items described in Attachments B1, B2, B3, B4, B5, B6, B7, and B8, and authorizing the seizure and examination of any such items found therein.


Special Agent Rachel S. Corn
Federal Bureau of Investigation

Subscribed and sworn to before me this 17 day of December 2018.


HONORABLE J. MARK COULSON
UNITED STATES MAGISTRATE JUDGE



18 - 3487 JMC

ATTACHMENT A1

DESCRIPTION OF ITEMS TO BE SEARCHED

(Digital Items Previously Seized)

The following items were seized from the person and residence of Kevin Daniel Mongold, Jr., on October 24, 2018, and are currently being held at the FBI, 2600 Lord Baltimore Drive, Baltimore, Maryland:

- *Black HP Laptop, Model: 15-BS020WM, S/N: CND72915HX*
- *White Apple iPhone, Model: A1453, IMEI: 352000068875701*
- *Black Apple iPhone with cracked screen, S/N: FCFTC10THG00, Model: A1661*
- *Rose Gold Apple iPhone, Model: A1687, S/N: F2M0M633GRWM*
- *Black XBOX 360, Model: 1439, S/N 406639703005*
- *Black Sony Playstation 4, Model: CUH-1115A, S/N: MB315941043*

18-3488 JMC

ATTACHMENT A2

DESCRIPTION OF ITEMS TO BE SEARCHED

(Cybertipline Reports)

Copies of associated files of Cybertipline Reports 11860995, 11861015, 42610198 and 42611405 that were forwarded to the National Center for Missing and Exploited Children (NCMEC) by Facebook and Box.com and are currently located within the State of Maryland.

18 - 3489 JMC

ATTACHMENT A3

DESCRIPTION OF ITEMS TO BE SEARCHED

(Facebook, Inc.)

This warrant applies to information associated with the following Facebook accounts:

- The Facebook account associated with the keviejrmongold@yahoo.com and the ESP User ID: 100010728783044;
- The Facebook account associated with the email address kevin.mongold19@yahoo.com, the ESP User ID: 100012201795245, and screen name: kevin.mongold.56;
- The Facebook account associated with the email address mongoldjr.kevin@gmail.com and the ESP User ID: 100017871872850;

that are stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company, headquartered at 1601 Willow Road, Menlo Park, California 94025.

18 - 3490 JMC

ATTACHMENT A4

DESCRIPTION OF ITEMS TO BE SEARCHED

(Oath Holdings, Inc.)

This warrant applies to information associated with the following Oath Holdings, Inc., accounts:

- keviejrmongold@yahoo.com;
- kevin.mongold19@yahoo.com;
- mongoldjim@yahoo.com;

that are stored at premises owned, maintained, controlled, or operated by Oath Holdings, Inc., a business with offices located at 701 First Avenue, Sunnyvale, California 94089.

18 - 3491 JMC

ATTACHMENT A5

DESCRIPTION OF ITEM TO BE SEARCHED

(Dropbox, Inc.)

This warrant applies to information associated with the following Dropbox, Inc. account:

- The Dropbox account associated with the email address:
mongoldjr.kevin@gmail.com and the ESP User ID: 721902735;

that is stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., a business with offices located at 185 Berry Street, Suite 400, San Francisco, California 94107.

ATTACHMENT A6

18 - 3492 JMC

DESCRIPTION OF ITEMS TO BE SEARCHED

(Google LLC)

This warrant applies to information associated with the following Google LLC accounts:

- mongoldjr.kevin@gmail.com;
- mongold.kevin@gmail.com;
- mongoldjim@gmail.com;
- mongold.kevin1997@gmail.com;

that are stored at premises owned, maintained, controlled, or operated by Google LLC, a business with offices located at 1600 Amphitheatre Parkway, Mountain View, California 94043.

18 - 3493 JMC

ATTACHMENT A7

DESCRIPTION OF ITEMS TO BE SEARCHED

(Box, Inc.)

This warrant applies to information associated with the following Box, Inc. account:

- The Box.com account associated with the email address mongoldjr.kevin@gmail.com and the ESP User ID: 2974294259;
- The Box.com account associated with the email address mongoldjim@gmail.com;

that is stored at premises owned, maintained, controlled, or operated by Box, Inc., a business with offices located at 900 Jefferson Avenue, Redwood City, California 94063.

18 - 3494 JMC

ATTACHMENT A8
DESCRIPTION OF ITEMS TO BE SEARCHED

(Apple, Inc.)

This warrant applies to information associated with the following Apple, Inc. accounts:

- The Apple account associated with the email address mongoldjim@gmail.com and DS ID 10032188562;
- The Apple account associated with the email address mongoldjim@yahoo.com and DS ID: 10031960637;
- The Apple account associated with the email address mongold.kevin@gmail.com and DS ID: 415693081;

that are stored at premises owned, maintained, controlled, or operated by Apple, Inc., a business with offices located at 1 Infinite Loop, Cupertino, California 95014.

FILED _____ ENTERED

LOGGED _____ RECEIVED

JAN 03 2019

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ DEPUTY

ATTACHMENT B1

18 - 3487 JMC

The items described in Attachment A1 may be searched for the following items, which may be seized:

All records, documents, items, data and other information that may constitute fruits or instrumentalities of, or contain evidence related to, violations of Title 18 §§ 2251(a), 2252A(a)(2) and 2252A(a)(5)(B) including, but not limited to, the following:

1. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18, U.S.C. § 2256(8).
2. Any and all correspondence identifying persons transmitting, receiving or possessing, through interstate commerce including by U.S. Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, U.S.C. § 2256(2).
3. Any and all records, documents, invoices and materials that concern any accounts, screen names, social networking sites, online accounts, or email accounts, including Internet Service Providers.
4. Any and all visual depictions of minors, to include depictions of minors engaged in sexually explicit conduct, nude pictures, and modeling.
5. Any and all documents, records, or correspondence pertaining to occupancy, ownership or other connection to 5403 Highridge Street, Halethorpe, Maryland 21227.
6. Any and all diaries, notebooks, notes, address books, pictures, emails, chats, directions, maps, banking, travel, documents, and any other records reflecting personal contact and any other activities with minors.
7. Any and all notes, documents, records, photos, correspondences that relate to travel.
8. Any and all notes, documents, records, photos or correspondence that indicate a sexual interest in children, including, but not limited to:
 - a. Correspondence with children;
 - b. Any and all visual depictions of minors;
 - c. Internet browsing history;
 - d. Books, logs, emails, chats, diaries and other documents.

As used above, the terms "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of

computer hardware, software, documentation, passwords, and/or data security devices.

9. For any computer, cell phone, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment; AND

j. image and video files that depict children engaged in sexually explicit conduct pursuant to Title 18 U.S.C. § 2256.

10. With respect to the search of any of the items above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

18 - 3487 JMC

- a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- c. "scanning" storage areas to discover and possible recover recently deleted files;
- d. "scanning" storage areas for deliberately hidden files; or
- e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

18 - 3488 JMC

ATTACHMENT B2

LIST OF ITEMS TO BE SEIZED

The items described in Attachment A2 may be searched for the following items, which may be seized:

Any and all files containing a visual depiction of a minor, to include images and videos of children engaged in sexually explicit conduct as described in 18 U.S.C. § 2256, nude pictures, and modeling.

Communication, information, pictures, videos or documentation that identifies the user of the account or that indicate a sexual interest in children.

FILED _____ ENTERED

LOGGED _____ RECEIVED

JAN 03 2019

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ DEPUTY

ATTACHMENT B3
(Facebook, Inc.)

18 - 3 4 8 9 JMC

I. Files and Accounts to be produced by Facebook between January 1, 2016, to the present.

To the extent that the information described in Attachment A3 is within the possession, custody, or control of Facebook including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to the **preservation requests made on October 24, 2018, and October 25, 2018, and assigned case numbers 2077256 and 2079899**, Facebook is required to disclose the following information to the government for each account or identifier listed in Attachment A3:

- a. All contact information, including full name, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, website, and other personal identifiers of the current status of the profile page and any individuals that have “defriended” them;
- b. All Photoprints, including all photos, videos and other files uploaded by the accounts listed in Attachment A3 and all photos, videos and other files uploaded by any user that have the accounts listed in Attachment A3 tagged in them, including all available metadata concerning these files;
- c. All Neoprints, including: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the User’s access and use of Facebook applications;
- d. All other communications and messages made or received by the user of the accounts listed in Attachment A3, including all private messages and pending “Friend” requests. All photographs, videos and other files sent and received in the private messages;
- e. All files and records or other information associated with the Cybertipline Reports 11860995 and 11861015;
- f. All IP logs, including all records of the IP addresses that logged into the account;
- g. All information about the User’s access and use of Facebook Marketplace;
- h. The length of service (including state date), the types of service utilized by the User, and the means and source of any payments associated with the service (including any credit card or bank account number);
- i. All privacy settings and other account settings;

18 - 3489 JMC

j. All records pertaining to communications between Facebook and any person regarding the User or the User's Facebook account, including contacts with support services and records of actions taken;

k. All communication to or from the user/subscriber of the account, including communication regarding the status of the account.

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the email accounts described in Attachment A3 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2251(a), 2252A(a)(2) and 2252A(a)(5)(B), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;
2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;
3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;
4. Images depicting the interior or exterior of residences, public establishments, and vehicles;
5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;
6. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;
7. Evidence of the times the account or identifier listed on Attachment A3 was used;
8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A3 and other associated accounts;
10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

18 - 3489 JMC

- b. All existing printouts from original storage which concern the categories identified in subsection II.A; and
- c. All "address books" or other lists of contact.

III. Search Methodology

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

ATTACHMENT B4
(Oath Holdings, Inc.)

18 - 3490 JMC

I. Files and Accounts to be produced by Oath Holdings, Inc., between January 1, 2016, to the present.

To the extent that the information described in Attachment A4 is within the possession, custody, or control of Oath Holding, Inc., including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Oath Holdings, Inc., or have been preserved pursuant to the **preservation request made on October 24, 2018**, Oath Holding, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A4:

- a. The contents of all e-mails, attachments and chat messages stored in the accounts described in Attachment A4, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;
- c. All internet search data including all queries and location data;
- d. All transactional information of all activity of the electronic mail addresses described above in Section I.A, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records or other information regarding the identification of the account described above in Section I.A, to include application, full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber, methods of connecting, log files, means and source of payment (including any credit or bank account number), and detailed billing records;
- g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;
- h. Flickr contents to include all images, videos and other files, and associated upload/download date and timestamp, including all available metadata concerning these files;

18 - 3490 JMC

i. Information regarding whether the Flickr files were private or public and who had access to view the private files;

j. Yahoo Messenger conversation logs and files shared associated with the accounts listed in Attachment A4.

k. Payment information, including billing address, shipping address, and payment instruments, associated with any Yahoo services used by the account listed in Attachment A4.

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the email accounts described in Attachment A4 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2251(a), 2252A(a)(2) and 2252A(a)(5)(B), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Images depicting the interior or exterior of residences, public establishments, and vehicles;

5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

6. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

7. Evidence of the times the account or identifier listed on Attachment A4 was used;

8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A4 and other associated accounts;

10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

18 - 3490 JMG

- b. All existing printouts from original storage which concern the categories identified in subsection II.A; and
- c. All "address books" or other lists of contact.

III. Search Methodology

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

ATTACHMENT B5
(Dropbox, Inc.)

18 - 3491 JMC

I. Files and Accounts to be produced by Dropbox, Inc.

Dropbox shall disclose responsive data, if any, by sending to the Federal Bureau of Investigation, 185 Admiral Cochrane Drive, Suite 101, Annapolis, Maryland 21401, ATTN: Special Agent Rachel Corn, or rscom@fbi.gov, using UPS or another courier service, or email, notwithstanding 18 U.S.C. 2252A or similar statute or code.

To the extent that the information described in Attachment A5 is within the possession, custody, or control of Dropbox, Inc. including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Dropbox, Inc., or have been preserved pursuant to the **preservation request made on October 24, 2018, and assigned reference number CR-7000-03554**, Dropbox, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A5:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, email addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- b. All information automatically recorded by Dropbox, Inc from a user's Device, including its software and all activity using the Services, to include, but not limited to: a utilizing device's IP address, browser type, web page visited immediately prior to connecting to the Dropbox website, all information searched for on the Dropbox website, locale preferences, identification numbers associated with connecting devices, information regarding a user's mobile carrier, and configuration information;
- c. The types of services utilized by the user;
- d. All files and records or other information stored by an individual using the account, including all images, videos, documents and other files uploaded, downloaded or accessed using the Dropbox service, including all available metadata concerning these files;
- e. All files and records or other information associated with the Cybertipline Report 41922524;
- e. All records pertaining to communications between Dropbox and any person regarding the account, including contacts with support services and records of actions taken;

18 - 3 4 9 1 JMC

f. For each folder within this account, all unredacted records including the unique user ids of each individual who created, joined or utilized the folder, by either adding content or deleting content from the folder;

g. A complete list of all users within each folder found in this account, including every user name, user identification number, corresponding email address, physical address, and date the user joined Dropbox;

h. Records of session times and durations and IP addresses associated with each of these sessions for every user in each folder in this account;

i. Telephone or instrument numbers provided to Dropbox when each of these users created their accounts, and records of all devices connected to the Dropbox accounts for each of the individuals accessing the folders in this account;

j. For each folder found in this account, all information regarding the user who created the folder, the creation date, and a complete listing of all users who joined, accessed, and left the folder, including the dates each joined, accessed or left the folder. All information regarding when, if applicable, each folder was deleted and who deleted it;

k. For the individuals identified as users of the folders in this account, any means or sources of payment for this service, including credit card and bank account numbers;

II. Information to be seized by Law Enforcement Personnel:

a. Any and all records that relate in any way to the Dropbox, Inc accounts described in Attachment A5 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2251(a), 2252A(a)(2) and 2252A(a)(5)(B), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Records or communication regarding who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

5. Images depicting the interior or exterior of residences, public establishments, and vehicles;

18 - 3491 JMC

6. All images, messages and communications, including any and all preparatory steps taken in furtherance of these crimes;
 7. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;
 8. Evidence of the times the account or identifier listed on Attachment A5 was used;
 9. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
 10. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A5 and other associated accounts;
 11. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- b. All existing printouts from original storage which concern the categories identified in subsection II.A; and
 - c. All "address books" or other lists of contacts.

III. Search Methodology

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

ATTACHMENT B6
(Google LLC.)

18 - 3492 JMC

I. Files and Accounts to be produced by Google LLC between January 1, 2016, to the present.

Google shall disclose responsive data, if any, by sending to the Federal Bureau of Investigation, 185 Admiral Cochrane Drive, Suite 101, Annapolis, Maryland 21401, ATTN: Special Agent Rachel Corn, or rscom@fbi.gov, using UPS or another courier service, notwithstanding 18 U.S.C. 2252A or similar statute or code.

To the extent that the information described in Attachment A6 is within the possession, custody, or control of Google LLC including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Google, or have been preserved pursuant to the **preservation requests made on October 24, 2018 and November 1, 2018, and assigned reference numbers 2132502 and 2147465**, Google is required to disclose the following information to the government for each account or identifier listed in Attachment A6:

A. Google Account Information

1. Google account registration information, including name, user-specified contact information, recovery email address, recovery SMS number, account creation timestamp and IP address, and a list of Google services the account holder has enabled or accessed;
2. Account change history IP addresses and associated timestamps;
3. Google account login and logout IP addresses and associated timestamps;
4. All means and sources of payment for all Google products and services (including complete credit or bank account numbers), and detailed billing records;
5. All cookie and user-specific advertising data, including third-party cookies;

B. Gmail Account Information

6. Gmail specific subscriber information, login and logout IP addresses and associated timestamps;
7. Gmail specific non-content email header information, originating message IP addresses, and account settings;
8. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

18 - 3492 JMC

9. Contents of all available deleted emails;

C. YouTube Account Information

10. YouTube specific subscriber information, including date of birth and country;
11. YouTube specific login and logout IP addresses and associated timestamps;
12. YouTube video upload IP addresses and associated timestamps;
13. Copies of all publicly available videos;
14. Copies of all private videos and associated video information;
15. Copies of all private messages;
16. All Channel or Video comments;
17. All contacts;

D. Google Voice Account Information

18. Voice specific subscriber information, including signup IP and associated timestamp and user-provided name;
19. Most recent 28 days of call and text logs;
20. All account settings and account change history;
21. Contents of all voicemail messages and text messages;

E. Blogger Account Information

22. Blogger specific subscriber information, including Blog registration information, Blog creation IP and timestamp, Blog owner/admin subscriber information, and post or comment owner information;
23. All contents of private blog posts and comments;

F. Google+ Account Information

24. Google+ specific subscriber and IP address information, including associated timestamps;
25. All IP addresses and timestamps associated with Posts, Comments, or Photos;
26. All Content/Activity Stream, including posts, comments, and photos;

18 - 3492 JMC

27. All contacts/Circles;

28. Google+ Profiles;

G. Android Account Information

29. Android specific subscriber and IP address information, including associated timestamps;

30. All device IDs, IMEIs, and MEIDs associated with the target account(s);

31. Timestamps, including device registration, first check-in, and last check-in;

32. All Google accounts tied to the Android device(s) if any;

33. Android hardware information;

34. Cell carrier/service provider;

35. All apps downloaded to the device;

H. Photos Account Information

36. Photos specific subscriber and IP address information, including associated timestamps;

37. All upload IP addresses and associated timestamps;

38. Contents of all Photos and Albums, including all exif data included by the user as part of the upload;

I. Drive Account Information

39. Drive specific subscriber and IP address information, including associated timestamps;

40. All upload IP addresses and associated timestamps;

41. All Drive content, including Docs, Sheets and Slides;

J. Google Location and Search History Information

42. All location history with associated timestamps between May 1-7, 2018, May 8-15, 2018, and October 18-25, 2018.

43. All search history and associated timestamps, including all "clicks" and "queries;"

K. Google Hangouts Account Information

18 - 3492 JMC

44. Hangouts specific subscriber and IP address information, including associated timestamps;

45. Hangouts specific non-content transactional information for all text, audio, and video communications, including originating message IP addresses, and account settings;

46. The contents of all Hangouts messages and attachments including images, videos and related timestamps and IP address logs;

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the email accounts described in Attachment A6 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2251(a), 2252A(a)(2), and 2252A(a)(5)(B), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Images depicting the interior or exterior of residences, public establishments, and vehicles;

5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

6. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

7. Evidence of the times the account or identifier listed on Attachment A6 was used;

8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A6 and other associated accounts;

18 - 3 4 - 9 2 JMC

10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

b. All existing printouts from original storage which concern the categories identified in subsection II.A; and

c. All "address books" or other lists of contacts.

III. Search Methodology

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

ATTACHMENT B7
(Box, Inc.)

18 - 3493 JMC

I. Files and Accounts to be produced by Box, Inc.

Dropbox shall disclose responsive data, if any, by sending to the Federal Bureau of Investigation, 185 Admiral Cochrane Drive, Suite 101, Annapolis, Maryland 21401, ATTN: Special Agent Rachel Corn, or rscom@fbi.gov, using UPS or another courier service, or email, notwithstanding 18 U.S.C. 2252A or similar statute or code.

To the extent that the information described in Attachment A7 is within the possession, custody, or control of Box, Inc. including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Box, Inc., or have been preserved pursuant to the **preservation request made on October 25, 2018**, Box, Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A7:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, email addresses, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- b. All information automatically recorded by Box, Inc from a user's Device, including its software and all activity using the Services, to include, but not limited to: a utilizing device's IP address, browser type, web page visited immediately prior to connecting to the Box website, all information searched for on the Box website, locale preferences, identification numbers associated with connecting devices, information regarding a user's mobile carrier, and configuration information;
- c. The types of services utilized by the user;
- d. All files and records or other information stored by an individual using the account, including all images, videos, documents and other files uploaded, downloaded or accessed using the Box service, including all available metadata concerning these files;
- e. All files and records or other information associated with the Cybertipline Reports 42610198 and 42611405;
- e. All records pertaining to communications between Box and any person regarding the account, including contacts with support services and records of actions taken;

18 - 3493 JMC

f. For each folder within this account, all unredacted records including the unique user ids of each individual who created, joined or utilized the folder, by either adding content or deleting content from the folder;

g. A complete list of all users within each folder found in this account, including every user name, user identification number, corresponding email address, physical address, and date the user joined Box.com;

h. Records of session times and durations and IP addresses associated with each of these sessions for every user in each folder in this account;

i. Telephone or instrument numbers provided to Box when each of these users created their accounts, and records of all devices connected to the Box accounts for each of the individuals accessing the folders in this account;

j. For each folder found in this account, all information regarding the user who created the folder, the creation date, and a complete listing of all users who joined, accessed, and left the folder, including the dates each joined, accessed or left the folder. All information regarding when, if applicable, each folder was deleted and who deleted it;

k. For the individuals identified as users of the folders in this account, any means or sources of payment for this service, including credit card and bank account numbers;

II. Information to be seized by Law Enforcement Personnel:

a. Any and all records that relate in any way to the Dropbox, Inc accounts described in Attachment A7 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2251(a), 2252A(a)(2) and 2252A(a)(5)(B), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Records or communication regarding who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

5. Images depicting the interior or exterior of residences, public establishments, and vehicles;

18 - 3493 JMC

6. All images, messages and communications, including any and all preparatory steps taken in furtherance of these crimes;
 7. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;
 8. Evidence of the times the account or identifier listed on Attachment A7 was used;
 9. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
 10. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A7 and other associated accounts;
 11. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- b. All existing printouts from original storage which concern the categories identified in subsection II.A; and
 - c. All "address books" or other lists of contacts.

III. Search Methodology

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.

18 - 3494 JMC

ATTACHMENT B8
(Apple, Inc.)

I. Files and Accounts to be produced by Apple Inc. between January 1, 2016, to the present.

To the extent that the information described in Attachment A8 is within the possession, custody, or control of Apple including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Apple, or have been preserved pursuant to the **preservation request made on November 1, 2018**, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A8:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments);

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy

18 - 3 4 9 4 JMC

lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. The activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the email accounts described in Attachment A8 which is evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. § 2251(a), 2252A(a)(2) and 2252A(a)(5)(B), specifically that relate to the following:

1. Images, videos and other files depicting the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

2. Communications or documentations regarding the production, distribution, receipt, possession of or access with intent to view child erotica, child pornography, the sexual exploitation of minors, sexually explicit conduct, and illicit sexual conduct;

3. Communication or documentation regarding access to and/or interaction with minors, to include the enticement of a minor;

4. Images depicting the interior or exterior of residences, public establishments, and vehicles;

5. All images, messages, communications, calendar entries, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

6. Communication, information, documentation and records relating to who created, used, controlled or communicated with the account or identifier, including records about their identities and whereabouts;

18 - 3494 JMC

7. Evidence of the times the account or identifier listed on Attachment A8 was used;
 8. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
 9. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed on Attachment A8 and other associated accounts;
 10. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- b. All existing printouts from original storage which concern the categories identified in subsection II.A; and
 - c. All "address books" or other lists;

III. Search Methodology

With respect to the search of the information provided pursuant to this warrant by the above-referenced provider, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically-stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable.